REMARKS

The non-final Office Action of September 26, 2005 considered and rejected claims 1-36.[1] Claims 1, 2, 4, 24, 26 and 30-36 were rejected under 35 U.S.C. § 102(b) as being anticipated by Deinhart et al. (U.S. Patent No. 5,911,143). Claims 19-23 and 25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Deinhart in light of the Examiner's knowledge of well known features in the art. Claims 3, 5-17 and 27-29 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Deinhart in view of Wong et al. "A Role-Based Access Control Model for XML Repositories."[2]

Claims 30 and 33-35 were further rejected under 35 U.S.C. § 101 as not being drawn to statutory subject matter for including tangible and non-tangible embodiments. Applicants note that claim 30 has been cancelled and that claims 33-35 have been amended to recite physical computer-readable media. Accordingly, Applicants submit that the rejection to claims 33-35 under 35 U.S.C. § 101 has been overcome and respectfully request withdrawal of the rejection based thereon.

In addition, claims 30 and 33 were objected to under 37 C.F.R. § 1.75(c) as being of improper dependent form. While claim 30 has been cancelled, claim 33 has been amended and refers back to, and further limits the method of claim 31. In particular, claim 33 limits the method of claim 33 by reciting that the recited act and step are performed by computer-executable instructions embodied within a physical computer-readable medium. Accordingly, Applicants respectfully submit that claim 33 is in proper form and the objection has been overcome.

[1] While the Office Action Summary indicated that claims 1-36 were rejected, no specific grounds of rejection were set forth for claim 18 in the Detailed Action, which only specifically addressed claims 1-17 and 19-36. As the grounds for rejecting claim 18 were not set forth, no response to the rejection of claim 18 is specifically offered herein. Nevertheless, in light of the other remarks herein, claim 18 is patentable over the cited references for at least the reasons presented.

[2] Although the prior art status and some of the assertions made with regard to the cited art is not being challenged at this time, Applicants reserve the right to challenge the prior art status and assertions made with regard to the cited art, as well as any official notice, at any appropriate time in the future, should the need arise, such as, for example in a subsequent amendment or during prosecution of a related application. Accordingly, Applicants' decision not to respond to any particular assertions or rejections in this paper should not be construed as Applicants acquiescing to said assertions or rejections.

By this paper, claims 1, 2, 10 and 31-36 have been amended, claim 30 has been cancelled, and new claims 37-39 have been added.[3] Accordingly, following this paper, claims 1-29 and 31-39 remain pending, of which claims 1, 31, 34 and 36 are the only independent claims at issue.

Applicants invention, as claimed for example in independent claim 1, relates to authorizing a requesting entity to operate upon data structures in a standard manner. The recited method maintains a plurality of role templates that define basic access permissions for one or more command methods. Further, such access permissions are further defined by the role templates in a manner that is independent of the type of data structure being accessed. The method also maintains a plurality of role definitions that define access permissions for requesting entities by using one or more of the role templates, and includes an act of receiving a request from the requesting entity to perform at least one of the command methods, while the request identifies the requesting entity. Further, a role definition corresponding to the requesting entity is identified, and access permissions for the requesting entity are determined with respect to the command method by using the role definition corresponding to the requesting entity. Additionally, the method may include maintaining a plurality of role definitions for the requesting entity, wherein the role definitions correspond to a plurality of authentication methods (claim 37), referencing a role template and refining, at a user level, a scope referenced in the role template (claim 38), or determining access permissions below the data structure level (claim 39).

Applicants' invention, as claimed in independent method claim 31, is related to the foregoing method, but is recited in functional (step for) language, while the invention as claimed in independent claim 34 recites a computer program product having physical computer-readable media storing computer-executable instructions for performing acts generally corresponding to the acts of recited in claim 1. Applicants' invention, as claimed for example in independent claim 36, is directed to a system for isolating the authorization process from the services so that the services need not independently authorize each request they receive. The system includes a plurality of services configured to facilitate operations on one or more types of data structures,

[3] Various amendments have been made merely to clarify the intended use of the invention and to correct minor informalities or grammatical errors (see, e.g. claims 1, 2, 31 and 34), and not for any reason related to patentability. Support for these amendments as well as other amendments and the new claims is found within the disclosure of Applicants' specification including at least the disclosure found in paragraphs [0007], [0009]-[0013], [0023], [0027], [0052]-[0063], [0079], [0080], [0085], [0090], as well as in the drawings, including Figure 3, of the originally filed application.

and an authorization station configured to receive, from a number of applications, requests to operate upon data structures with any of the number of services. As further recited, the authorization station is configured to receive a request from a requesting entity to perform a target operation upon a target data structure managed by a target service, and as clarified by the above amendment, access role template that defines basic authorizations with respect to one or more operations which include at least the target operation, wherein the role template defines the basic authorizations in a manner that is independent of the target data structure desired to be operated on. The authorization station then determines that the corresponding requesting entity is authorized to perform the target operation on the target data structure, and communicates that authorization to the target service.

As noted above, independent claims 1, 31, 34 and 36, and dependent claims 2, 4, 24, 26, 32-33 and 35 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Deinhart. While Deinhart appears to generally disclose methods and systems for authorizing and controlling access rights in a computer system, Applicants respectfully submit that the cited art fails to anticipate or make obvious the claimed invention. For example, the cited art fails to disclose or suggest, among other things, a method, computer program product, or system wherein any role template defines basic access permissions for one or more command methods in a manner that is independent of the type of data structure being operated upon. In other words, the cited reference fails to disclose or suggest a role template which defines operational authorizations in a manner that is detached from the object being accessed.

In fact, Deinhart appears to disclose a template which defines basic operations expressly based on the type of object being accessed. In particular, Deinhart teaches that a role type is used to control and authorize access rights to objects of various resource types, including files, disks, displays, printers, scanners, and transactions. (Col. 3, ln. 30-34). The role type acts as a template by combining a set of functional tasks with a generic set of competencies, and does so by defining not only access rights, but also objects and transactions. (Col. 3, ln. 54-58). For example, and as illustrated in Figure 2C, a role type (e.g. Role Type 2) is depicted which defines access rights (e.g. use) *and* associates that access right with an object type (e.g. printer). Accordingly, Deinhart appears to teach a role type which, while acting as a template, defines generic competencies and access rights as they specifically and expressly relate to generic object types (col. 8, ln. 66 to col. 9, ln. 1), and fails to teach any role template that defines basic access permissions in a manner that is *independent of the type* of structure being operated upon, as claimed. As a result, Deinhart fails to anticipate claim 1 of the present invention, particularly in combination with the other recited claim elements.

It will be appreciated that independent claims 31, 34 and 36 incorporate similar limitations and that although only claim 1 has been specifically addressed, for at least the foregoing reasons, Deinhart also fails to anticipate independent claims 31, 34 and 36. Moreover, because all independent claims are allowable over the cited reference, it will also be appreciated that all other rejections and assertions of record with respect to the other dependent claims are now moot, and therefore need not be addressed individually. However, to further differentiate between the cited references and the present invention, a few dependent claims will be addressed specifically.

With respect to claim 2, while Deinhart discloses determining access permissions, Deinhart fails to disclose an act of the role definition corresponding to the requesting entity using at least one access permission that is specific to the requesting entity, as claimed. For example, while users may each have a user identification (col. 10, ln. 35-40), role instances define a user's access permissions for specific, concrete objects based upon only the user's general role type, job position, and organizational unit. (See Figure 3C). In other words, access permissions are based on the organizational structure and are not specific to any particular user, as claimed.

With respect to claim 10, the Examiner has acknowledged that Deinhart fails to teach a role map document (see Office Action, page 12 discussing claim 5) and therefore also does not disclose defining a role definition by referencing a role template included in a role map document. To supply this element, the Office Action cites the Wong reference. Applicants respectfully disagree, however, that Wong recites such an element. In particular, Wong appears to disclose a single configuration file which consists entirely of descriptions, a single role-tree, users, SSD, and DSD. (Pages 143-144). Users are defined by a user-name, password, and an optional RolePointer, which points to a role found within the role-tree also defined within the configuration file. (Id.) Accordingly, Wong discloses that the RolePointer references a role within the same file, and fails to disclose a role definition referencing a role template included in a distinct role map, as claimed. Further, Applicants note that the RolePointer is included within a *user* definition and is not a *role* definition referencing a role template, as recited in claim 10.

With respect to claim 37, Deinhart and Wong fail to disclose role definitions which correspond to a plurality of authentication methods. In particular, Deinhart appears to teach that various role instances are synthesized which define competencies bound to specific role types based on organizational units, and capability lists are created and which identify access rights to objects on a per-user basis. (Col. 3, ln. 60-64, col. 8, ln. 12-15; abstract) Deinhart fails, however, to disclose either a plurality of authentication methods or role definitions which correspond to a plurality of *authentication methods*. Similarly, Wong fails to supply these recited elements. In particular, Wong discloses at most a single user identification method in which a user is defined by a user ID and password. (Page 144). Accordingly, Wong also fails to disclose a plurality of authentication methods, let alone role definitions corresponding to the plurality of authentication methods, as claimed. Accordingly, Deinhart and Wong, both singularly and in combination, fail to teach or suggest the present invention as recited in claim 37.

With respect to claim 38, the cited references fail to disclose, among other things, refining a scope at a user level. In particular, Deinhart appears to teach that parameters may be used to modify generic capabilities, but that such parameters are provided based on job position or organizational unit (col. 4, ln. 18-36). Accordingly, Deinhart teaches that the modifications occur at organizational levels, rather than at the user level, as claimed. Wong also fails to provide at least this same recited element. In particular, Wong discloses a university system in which various categories of personnel are specified (e.g. staff, students, etc.). (Pages 143-144). Wong fails to disclose, however, any refinement of a role template, let alone any refinement at a user level and, accordingly, fails to teach or suggest the elements as recited in claim 38.

With respect to claim 39, Deinhart and Wong also fail to teach or suggest the invention of the recited claim. For example, Deinhart and Wong fail to disclose determining access permissions below the data structure level. In particular, while Deinhart and Wong may disclose accessing or controlling a file or other object, the cited references fail to disclose that the permissions are determined below the data structure level, as claimed, and particularly in combination with the other recited elements.

In view of the foregoing, it is respectfully submitted that all claims should now be found in condition for prompt allowance over the cited references. In the event that the Examiner finds any remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney.

Dated this 9 day of December, 2005.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
JENS C. JENKINS
Registration No. 44,803
Attorneys for Applicant

Customer No. 47973

JCJ:CCN:ppa
CN0000000128V001